NETWORK CENTRIC WARFARE FOR COALITION INTEGRATED DEFENSE AGAINST TERRORISM

Eric C. Firkin,
Raytheon Solipsys
6100 Chevy Chase Drive,
Suite 200
Laurel, MD 20707
eric.firkin@solipsys.com

Margaret M. McMahon, Ph. D.
Computer Science Department, US Naval Academy
Annapolis, MD
mmmcmahn@usna.edu

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 2004		**00-00-2004 to 00-00-2004**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Network Centric Warfare for Coalition Integrated Defense Against Terrorism	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Raytheon Solipsys,6100 Chevy Chase Drive Suite 200,Laurel,MD,20707**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**35**	

Abstract

The tragic events of 9-11, terrorist actions in Russia and the Philippines, along with cancellations of several international civilian air flights, have brought the world closer in forming an alliance pitting industrialized nations against less technically advanced, but extremely dedicated, international terrorists. The ability to operate as independent nations in this fight against loosely defined organizations requires a tightly netted collaboration of military and inter-governmental organizations working as a single entity, while maintaining some level of national independence.

Through the use of a demonstrated Network-Centric Warfare (NCW) solution, called Tactical Component Network (TCN), countries exchange information among designated mission-centric groups with the distribution of data and its fidelity determined by the data's owner. TCN can use a local environment for small real-time operations or a global hub network that will integrate coalition partners in a shared network of sensors and intelligence information.

TCN allows individual nations' stove-piped systems to share data, common pictures, and intelligence information for any region of interest. The TCN architecture has successfully been demonstrated by the United States military in a variety of stressing applications. To facilitate the detection and neutralization of terrorists, this same infrastructure can support multi-national applications.

Relevance to Network Centric Applications

Recent worldwide events have shown that traditional concepts for defending a nation's borders and its populace must be modernized to react to current threat scenarios. Terrorist organizations do not honor the borders of countries, so that the old ways of combating these threats must be modified. Countries must be willing to share military and intelligence information with their neighbors on common networks. However, sometimes the source or fidelity of that information may still require protection; networks need to be able to provide methods for distributing information among a group of coalition partners in a way that protects the provider's national interests while supplying data to meet the needs of a multi-national mission-oriented application.

The Tactical Component Network (TCN) provides the ability for command authorities to form a common representation of a mission application in real-time at the local, national, or regional level, hence increasing the effectiveness and speed of the decision timeline. TCN integrates diverse capabilities into a collaborative system allowing participants to transfer information in a uniform manner across a diverse set of communication paths. TCN has it genesis in the world of complex sensor networking, where a variety of different sensor types with different precisions and capabilities form a cohesive track picture. While users broadcast their needs to all within the shared collaborative network, the specific needs of each individual user are met by tailoring the track picture. The collaborative data gained from the sharing is in the form of Current Observation Related Estimates (CORE), which essentially contains the error coefficients associated with the measured event they are reporting [1]. This allows a user to combine this data with local data on the same entity to refine the local understanding of the reported event. For example, Coalition partners participating in the integrated defense network would share common airborne and ground track numbers, intelligence and maritime information, and coordinates and inputs from first-responder groups of terrorist actions. Each user will synthesize the data to meet their local requirements and request the data required toward this goal. The result is that each user attains the tailored representation of information that meets a specific mission-centric need.

Tailoring the data to the mission is a key aspect of the TCN approach. There are fundamentally different needs for each user, even with the same mission area. For example, the data to engage and destroy an incoming missile by a low altitude air defense system is different from higher echelon situational awareness. In an air control environment, the needs of a commuter knowing

when his or her flight is due to arrive are different from the air controller directing the final approach phase for multiple aircraft. However, the source of the data may be the same in some instances.

In situations where data may have restricted access, the "producers/owners" of information can control access, thus ensuring that national capabilities or contributors are not compromised. Although some data has restricted access, reach-back capability for added support in crisis situations is quickly assessable. Remote expertise can be rapidly tapped without being forced to bring all resources directly to an area where a dangerous situation may be in progress. The interface between the local and global communications networks is seamless to the end-users and information sources allow data to be transferred in a real-time environment without compromise to contributors.

The Solution

TCN is an enabling technology with architecture that allows for the transparent integration of sensors, processors, and communications assets in a network environment to enable diverse functions to operate as a single unit without effecting their individual mission execution [2]. The versatility of TCN enables its operation in many different environments and deployment options. Small operations are normally accommodated by what is defined as a TCN Local Network. This TCN Local Network will handle the real-time execution of time sensitive data. The second deployment option is a Wide Area Network (WAN) capability called the TCN Global Network. The Local TCN network allows the individual peer networks used by police, medical, intelligence, and military teams to interoperate in a real-time arena. This coordination is implemented by the TCN Global Network, capable of melding multiple TCN Local Networks into an integrated single network. A single Hub can be established for an individual theater of operations, or multiple nodes may be utilized depending on the amount of data and level of network fidelity and communications paths. Users may be large command centers, ships, aircraft, police vehicles or individual users equipped with Personal Digital Assistants (PDAs). The data transmitted is typically data that is observed and can be characterized by its error coefficients. Applications or Components as they are known in TCN synthesize the data into a representation that is mission-centric and needs-based.

TCN provides an open-architecture approach to creating a network-enabled tactical environment at the fidelity required, and delivers information to users based on their specifications for mission execution [2, 3]. When developing these networks, the structure and architecture should be driven by the "missions needs" and not by just the current network capability. These mission-centric networks then supply data information knowledge to network consumers while minimizing the bandwidth requirements on landline and wireless communication links [2]. To minimize both data distribution on the network, as well as the processing requirements of participating systems, the "needs" of an individual user drive data distribution bandwidth. Rather than distributing all data to all participants in the network, data users receive the types of data for which they register. Processing load is reduced because of fewer input interrupts. Data is also throttled by the network itself, so that no data is sent that does not contribute to meeting a need. For example, a commercial aircraft flying straight and level at a known speed requires fewer position updates than does the same aircraft turning out of its airway and heading for a known terrorist target.

TCN is based on users pulling data that meets their precise needs to accomplish varied missions, so that one can envision hundreds or thousands of end-users obtaining the information they need at the proper fidelity and time. TCN not only supports well connected users known as "advantaged users", but also the "disadvantaged users" who may need to obtain information quickly on a narrow bandwidth network. Some examples of a disadvantaged user's need for the network could include: a motorcade, which might require a surveillance picture of the immediate airspace and roads in the area with alternate routes; or high value-targets, such as nuclear power plants and sports stadiums that need surveillance data for the immediate area in time to make a proactive response to a terrorist threat, both being done over a wireless network which is completely mobile.

One of the greatest inhibitors to effective law enforcement is the inability to get information to front-line patrol personnel or border inspectors in a near real-time environment and then providing a way for them to add amplifying information. Using a TCN based network, police or customs personnel could request immediate information from intelligence databases on individuals that seem suspicious, but have not committed any type of crime. Their location could be entered in a database to include amplifying data such as vehicle type, license plate

number, and physical characteristics. This could be done on a PDA utilizing a cell phone network. Another application might entail providing information to first and second responders prior to their arrival on site. In a terrorist hostage or sniper situation, information on locations of terrorists could help to formulate a response prior to arrival. Information on building designs or security could be downloaded from databases located many miles from the scene and available to Special Weapons and Tactics (SWAT) personnel. With a common infrastructure for the logical exchange of information, individual or networked Components can add value to each mission area by potentially using the same data in different ways than other Components.

The Tactical Component Network

TCN technology transparently integrates sensor and communications suites with distributed network applications [4]. A sensor could be anything from an air defense radar tracking thousands of targets to an unattended ground sensor detecting a single tank, or an eyewitness observation to a terrorist sighting. It is an enabler for time-critical, needs-driven applications where automated collaborative solutions are required from many users working with diverse sources of information [5]. The ingenious capability of a TCN solution is that it accommodates legacy systems and facilitates an orderly migration to a well-defined component architecture that can be maintained and extended [3, 4].

The TCN Local Network component handles the time-critical, peer-to-peer applications, while the wide-area capability is handled under the TCN Global Network. The local TCN network provides the fabric for network-centric grids; it allows the individual peer networks used by dissimilar teams to interoperate in a given geographic area. Wide-area coordination can then be facilitated by a Hub-and-Spoke architecture tying local geographic networks into a global network; this capability is implemented by the TCN Global Network [5].

Hub-and-Spoke Architecture

Local networks can be limited in range and by technology. The Hub-and-Spoke architecture provides a means by which local TCN networks can interact with each other and stored, value-added information. Through the use of a Hub, local entities are provided a global reach, participating in a multi-tiered global information grid. The connection of Local TCN networks to the Hub is shown in Figure 1 [3, 5].

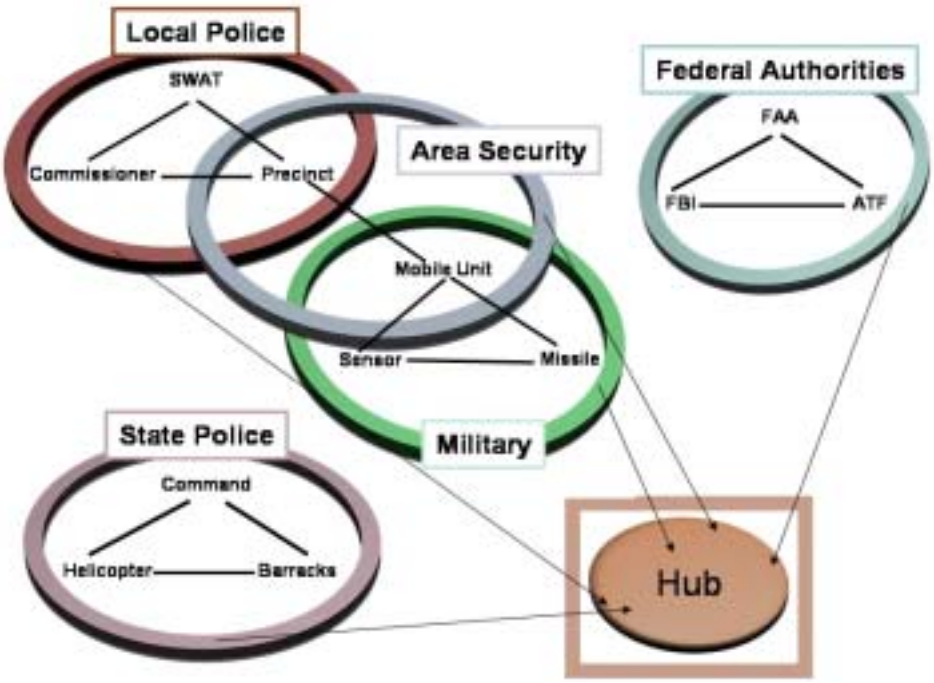


Figure 1 - Local and Global TCN

The TCN open-architecture approach supplies data to network consumers while minimizing the bandwidth requirements on landline and wireless communication links. Network users monitoring the same event only send a data update when it is required to meet the accuracy needs of the most demanding network segment user. For example, if it was desired to know where a person was within a 10 meter radius and the person moved a meter from the current position and was observed, no data needs to be sent. However, an observation that the person moved 11 meters from the last known location would be sent by the first "sensor" observing that event. In this way, data is said to "earn" its way on the network and not just chatter to clog the network. Communication devices are key participants in this process, whereby both sensors and communication devices on a network segment each are equipped with a software application called a Data Conditioner. Data Conditioners on a Local Area Network (LAN) communicate locally and with all other data conditioners accessible in the current instantiation of TCN. In the simple example above, if a segment had two sensors and one communication device, and one of the two sensors had a more recent observation than one currently in the outgoing communication queue, it would automatically replace the older data with the new before the transmission gate was reached. This, among other things, reduces the processing load of receivers, because fewer

input interrupts are received and all data is in a universal coordinate system. This enhances data registration and local processing capabilities. In a TCN-enabled architecture, each sensor and all communication devices act in concert to create a collaborative picture of the environment. While used most often for creating a single integrated air picture, TCN can be applied to any discipline where the uncertainty of remotely sensed data can be characterized analytically [2]. Figure 2 demonstrates a military application of Beyond-Line-of-Sight (BLOS) TCN architecture utilizing the Iridium satellite constellation. Three completely diverse levels of mission execution are shown collaborating in a Global TCN network each sharing information with each other, but only receiving the level of information and fidelity to execute their portion of the mission. Participant C has a much smaller field of regard then participant A and B, so that the bandwidth required to support participant C is smaller.

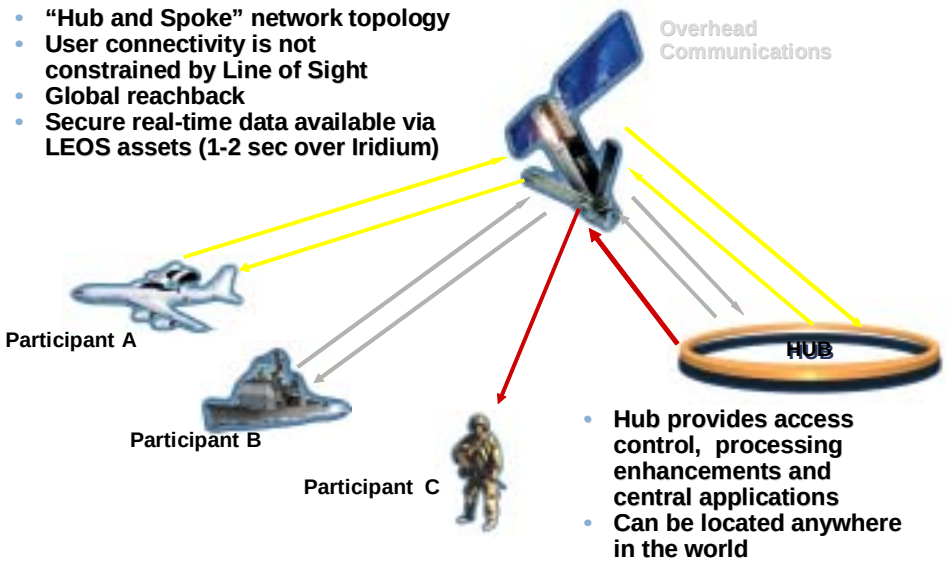


Figure 2 - Military Application of TCN BLOS Architecture

TCN Architecture Overview

For a mission-centric network to meet each user's needs, it should conform to the seven cornerstones of sensor networking at a minimum [3]. The seven cornerstones are the following:

- Network extensibility must be minimally impacted by the number of network participants.
- Network participants must maintain physical and functional independence.

- Each network must be responsive to diverse user needs.
- Network data communication structure must seamlessly include all wireless data paths.
- Multi-level data access must be supported. Sensor elements must act in concert to meet user-specified objectives.
- All element-specific processing must be performed at the originating elements and not at the recipients.

TCN addresses all seven in an open-architecture environment. TCN has, as its foundation, a collection of generic software applications including Data Conditioner, Current Observation Related Estimate (CORE) Synthesis, reporting needs management, Multi Source Correlator Tracker (MSCT), Visualization (Tactical Display Framework [TDF]), and Messaging. A notional TCN structured is shown in Figure 3 [1, 2, 3].

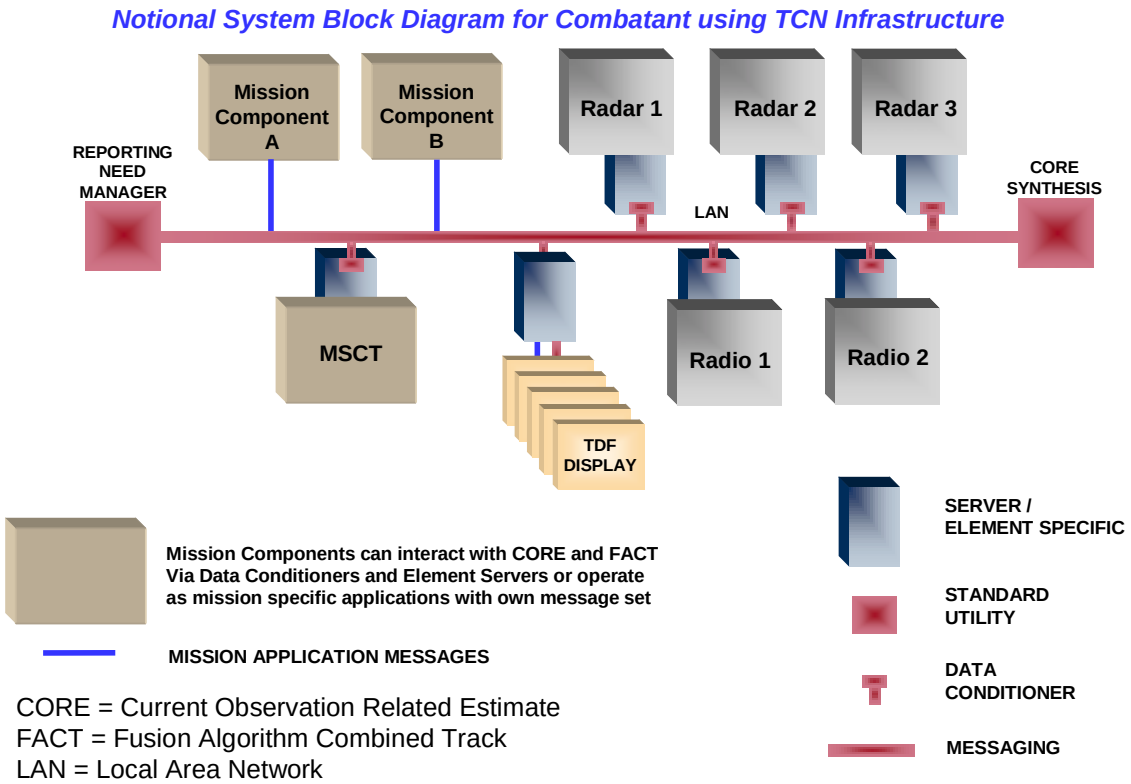


Figure 3 - TCN Segment

Within the TCN framework, the network processes are decomposed into common components. The components are designed so that data sources and consumers can be added without changing other components in the network. Standard utilities link the dissimilar data sources with

consumers. As shown in the notional diagram above (Figure 3), some components called servers connect legacy devices to the TCN infrastructure. The servers are designed specifically to couple a non-TCN device into the TCN infrastructure, so that they are able to exchange data with other TCN Components. In newer systems, the server functions can be built directly into the device. TCN-networked sensors exchange information with the rest of the network through a Data Conditioner. The Sensor Data Conditioner (SDC) accumulates and condenses the data into CORE. The SDC provides the data to the network based on the user-defined needs level of the track. Local CORE Synthesis then fuses the CORE with the appropriate network track and distributes a FACT to all users on the segment that have requested and have been approved for the specified track data. Data Conditioner and CORE Synthesis are standard network utilities common to all segments, while the Sensor Server is a network component unique to the sensor [1, 3]. Through components such as visualization (TDF), legacy-system tracking, and correlation (MSCT), value-added services for threat evaluation or identification can be attached to a local segment or a TCN Global Network Hub. This also allows legacy, non-TCN-equipped participants to interact with TCN participants and allows for a smooth transition during the TCN fielding process [2].

TCN architecture is an operational architecture with many of its components employed by the U.S. Navy and Air Force; it can be adapted to meet the challenging demands of coordinating dissimilar national assets as well as diverse international efforts.

Extending TCN

TCN implements a suite of components that can not only be tightly coupled to produce a single, integrated system, but also implemented independently, or in stages as funding or needs dictate. These individual components have been developed modularly, with key parts implemented in separate components. The existing TCN components can be extended by third-party developers, by implementing new applications that will be integrated into TCN. This allows users to develop their own customized applications to better suit their needs.

The Hub

The Hub-and-Spoke configuration is similar to a municipal telephone system, where the Hub acts as the telephone central office. The Hub is an automated, value-added redistribution point for collaboration. The Hub provides a means of worldwide connectivity to a diverse set of missions and potentially to coalition partners. A Hub is a centralized concept; however, the Hub functions can be replicated to prevent having a single point of failure. Links to the Hub, as well as the Hub, can be redundant to maintain communication capability.

Persistent data can be maintained at the Hub and provided to users via a validated request. Users may be requesting specific data or may subscribe to a data service. The Hub maintains and controls publisher and subscriber associations, as well as data access controls. Through the Hub, “owners” of information can control any user's level of access. This allows multi-national and multi-organizational teams to share data without compromising operational capabilities.

The Hub also contains a real-time repository of historical and current data. It provides an integration point for evolving revolutionary value-added applications. The Hub can also provide for planning and simulation of operations.

Hub Roles

The Hub can serve as an information destination, an information filter, an intermediate point for the flow of information, or a gateway to other services.

As a destination, the Hub stores data and provides appropriate data access to all subscribing platforms. Storing data at the Hub, allows users to access to data asynchronously. For example, the precise identification and location of dangerous areas could be stored at the Hub and available to users as they join the Hub. Updates about the status of the areas could be published to subscribing users as they become available. Inherent in the Hub is an intelligent store-and-forward function for users with intermittent connections; the current relevant information can be transmitted when a previous connection is reestablished [5].

In its role as a filter, the Hub provides data that is tailored for the users, at the level they require, and in accordance with their status in a diverse environment. Individual platforms may be more concerned with access to only certain types of area data. For example, mobile ground-based

equipment has a more urgent interest in land mine data than an aircraft does. Additionally, it might be inappropriate for all participants in an emergency response operation to receive information about evolving agency enforcement actions that are sensitive.

When serving as an intermediate point, the Hub links local line-of-sight (LOS) networks of communication and sensor systems. Data can be passed between the users of separate physical networks, allowing them to seamlessly become users in a global network. Extension of the local networks allows better communication between users of different organizations, and between different units within the same organization. Additionally, the Hub passes only the information that improves the local awareness requirements stated by each user.

The Hub can serve as a gateway to other services. The data collected from all Hub users could be sent to artificial intelligence and operational analysis applications. The output from those applications would benefit all users when optimizing the deployment of critical resources.

The major roles of the Hub are shown in Figure 4. The resident applications are the heart of the Hub. Data is shown entering from the left. Incoming data is first processed at the Hub and then the resulting information may be stored for future use, sent to users, transferred to resident experts, and/or transferred to other services.

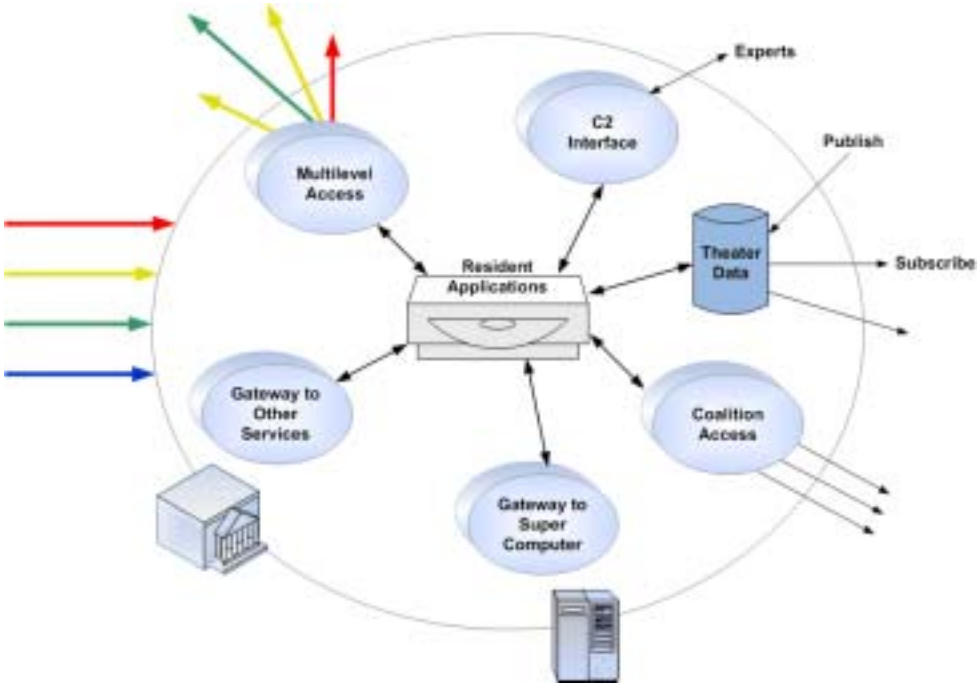


Figure 4 - Major Roles of the Hub

Hub Features

The Hub is a central point for hosting centralized applications and data exchange. The spokes of the Hub can provide communication links more reliably than LOS systems in some circumstances, so that participants can respond more quickly to changing situations. Better communication translates to less chance of users inadvertently interfering with other participant's objectives whether through ignorance, or use of obsolete data.

The Hub stores information in a persistent database. This is a repository for the corporate knowledge of users in the region. Information will be available to authorized subscribers who request notification, and to users upon joining the network. Information can be customized for the users' needs and level of access [5]. Senior personnel, experts, and analysts can be stationed at the Hub and can use it to communicate decisions to network users.

Input and output information for the Hub may be of varying bandwidths, and various technologies. Each user can interact with the Hub on its own particular link. Examples of specific input and output technologies are Iridium phones, T-1 lines, Public Switched Telephone Network (PSTN), or a dedicated T-3 line to a Super Computer Center. By installing receiving and transmitting hardware/software on the Hub, a connection of any type is possible.

In an operational environment, redundant Hub sites are required to ensure continuous service. Migration to a back-up Hub will occur when an error state exists, or there is loading beyond specification limits. A protocol will keep back-up Hub(s) informed of the current state of connections and services. The data may be transmitted periodically, or as spokes into the Hub become active or inactive. In the event of a fail over, or to recover from a power failure, this data regarding the current configuration ensures a seamless transition of service.

The security of the transmissions is provided by encryption. In the case of sensitive operations, only encrypted traffic will pass between users and the Hub, or between Hubs. This requires a bank of encryption and decryption devices that may be unique to specific applications or communication services. Management of Keying Material (KEYMAT) is a significant challenge in Hub operations and must be handled in accordance with certified procedures. Physical security is also required and is implemented at all Hub sites. A proposed Hub logical configuration is shown in Figure 5.

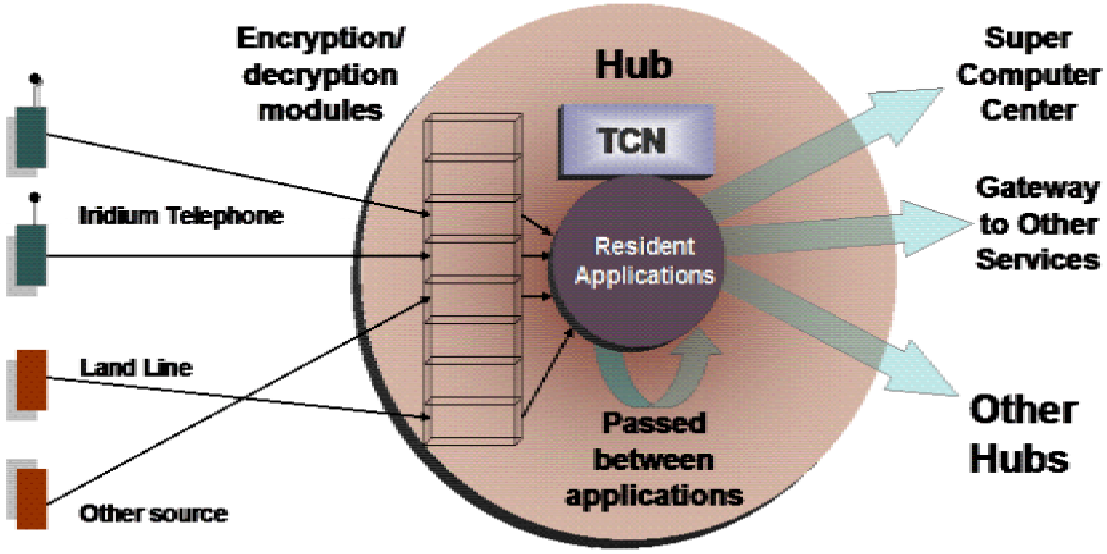


Figure 5 - Proposed Logical Hub Configuration

Hub Applications and Components

Applications that require large amounts of data and processing power are not typically implemented in fielded systems. The Hub can support algorithms that also combine all users' data with information not available to individual users. Such algorithms could also include use of operational, regional, and global operation goals. An example application would be to determine pairings of users' assets based on availability and operation-wide objectives; this knowledge is typically outside immediate knowledge of each individual user.

Rapidly evolving situations would benefit from near-real-time radio frequency (RF) planning applications. Creating a plan for frequency allocation can be intensive for computing resources, so that it is impractical for fielded systems to devote resources to respond to changes such as users vacating a frequency range. An RF planning application run on the Hub could assist in reducing RF interference in a critical area, without taxing the processing of local computing systems.

The development and testing of Hub applications primarily affects only the Hub. Adding or updating applications should produce minimal impact on any Hub users, requiring only a small amount of integration testing. To further reduce the impact on Hub users, any client/server interaction will use thin clients that require little or no maintenance on users' systems.

The Hub's operating system is embodied in several processors and is tasked with starting the Hub functions, and is responsible for monitoring the health of software components and itself. The Hub acts as a decision point or supervisor for what data is sent to each spoke. The Connection Manager is a network function distributed throughout TCN that automatically manages dissemination of publisher/subscriber data, access control, and the collaborative features of sensor data. The Database Manager is associated with determining which static databases have information useful to subscribers and in some cases must reach out to obtain additional data required by an end-user [5]. The components of the Hub are shown in Figure 6.

Figure 6 - The Hub Components

Hub Use in an International Environment

The Hub-and-Spoke architecture is essentially designed to provide both a wide-area and tactical, near real-time network for time-critical data with the Hub acting as a concierge ensuring that the needs of each user are relentlessly satisfied. Users can be connected via many different communication nodes to include landline, satellite, or cell-phone communication and benefit from the aggregate data available on the Hub. The Hub also serves as a gateway to existing databases or to resources external to its network. Each spoke of the architecture is designed to meet that spoke's user needs, so it is not difficult to interface an individual nation's stove-pipe

systems with the Hub, thus providing it with new information and data sources that were not previously available. This also allows different nations to share a common area picture by providing a gateway between the different systems. This combination of data allows for coalition-partner data to be shared in a common, easily assessable database. Combining intelligence data, from sources that in the past would have been separated, could help in the determination of intent of a terrorist group leading to their neutralization prior to execution.

Because of the Hub's access control capability, users are able to share intelligence information to include SIGINT and HUMINT reports without compromising their individual systems or sources capabilities. Each spoke can also be secured to the level of security classification data that is carried on that spoke. By sharing and integrating this information into a "needs-based representation", previous reports or inputs that might not have been seen as significant combined with inputs from other areas, may be the key piece of data in preventing a terrorist attack. Rather than send all data, and have every participant in the network replicate all the processing to determine a common understanding of the environment, TCN only distributes information that improves the representation held by each user. This dramatically minimizes individual components processing time and conserves bandwidth.

In many situations, continued interface with the Hub will not be available. In these instances, short dial-in or Short Burst Data (SBD)-type connections can be used to exchange small amounts of data. This capability could be very important to disadvantaged users who find themselves in a situation where continuous communications emissions are either not available, or are mission prohibitive.

Figure 7 shows expanded capabilities from the capabilities shown in Figure 1. In this figure, the networks of three different coalition partners demonstrate how the TCN architecture can be scaled to meet more of an International or Coalition-type scenario where participating countries interact with each other on a single, mission-centric network. The basic architecture does not change as the number or distance between participants is increased.

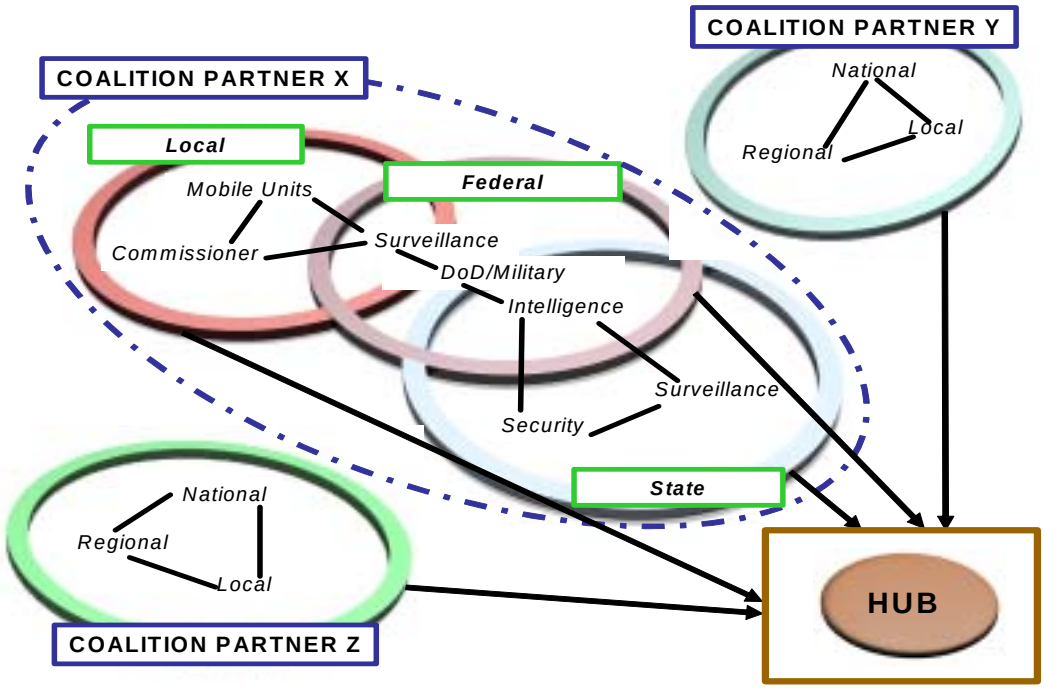


Figure 7 - Joint Coalition Partners

Hub Performance

Tactical Component Network (TCN) data from the initial implementation of the Hub applications in Kauai, Hawaii, was collected and analyzed. Four data runs were made: two in each direction, between a simulated ship and the Hub in Kauai. The first and second data runs were done simultaneously, as were the third and fourth. Network time synchronization was possible using the Iridium's built-in clock. The data was reviewed to verify that the packet sent had been received. Combining the results of the four experiments resulted in an average end-to-end delay of 2.51 seconds. The results are shown in Table 1.

Table 1- Results of the Four Experiments (in seconds)

	Hub-Ship (1)	Ship-Hub (1)	Hub-Ship (2)	Ship-Hub (2)	All Points
Average	2.35	2.32	2.74	2.69	2.51
Std Dev	1.69	1.29	2.29	2.05	1.84
Data Points	449	448	331	431	1659

Differences between the pairs of measured delay suggest that Iridium network might have been more heavily loaded during the second data run. These values compare favorably with known performance. The technical aspects of these tests are discussed in [4].

Current TCN-enabled Applications

TCN is currently installed in several ships of the US Navy's 7th Fleet and also has been interfaced with E-2 and P-3 airborne surveillance assets. This architecture was also implemented for exercise Foal Eagle 2002 and Cobra Gold 2002/4. Figure 8 shows several levels of networks that performed successfully during exercise Cobra Gold 2002. LANs connect TCN elements on a platform; wireless networks connect platforms within LOS of the radios; and a WAN employing TCN Global Network technology, utilizing the Iridium satellite constellation, can connect any platform, anywhere, anytime [2, 3].

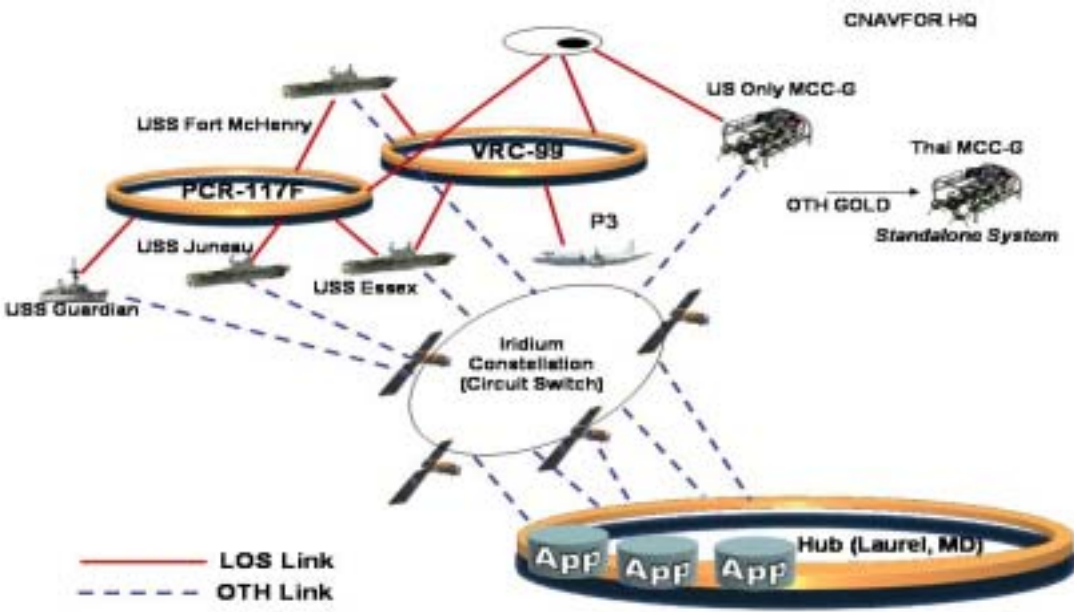


Figure 8 - Cobra Gold 2002 Configuration

This same basic architecture could be deployed in an international scenario without modifications. Command centers could share information among different internal users using standard LAN connections. Local DoD players could share information across standard UHF radio waves through the TCN network or by Link-16 using TCN's MSCT gateway. Local police,

firefighters, and other first responders could have the information distributed via wireless communications directly into a laptop or PDA in their patrol cars and command vehicles. Figure 9 is an example of an air picture shown on an iTAC PDA system.

The iTAC allows disadvantaged users the ability to participate in a TCN network while on the move. It has the same "look and feel" as the standard PC based TDF with high resolution geographic and landmark features including terrain, cities, boundaries, FAA flight routes, special use regions and airspaces, road, grids, rail lines, etc. Users can also display imagery from intelligence databases and weather from national weather services that would be valuable in a chemical or nuclear attack.

Figure 9 - iTAC PDA and Screenshots

During a time of crisis, when power for local cell phone towers and thus communications might be lost, users could still be a part of the network by using the Iridium satellite network, which would be unaffected by local power outages.

After the events of 9-11, North American Aerospace Defense Command (NORAD) selected two components of TCN (MSCT and TDF) to immediately eliminate its greatest shortfall in US air defense by integrating the FAA CONUS internal radar into the NORAD air defense system [6]. The NORAD Contingency Suite (NCS) was deployed to NORAD's three Sector Operations Control Centers (SOCC) and its Air Operations Center (AOC). NCS is still operational today at all four locations [4]. Those two components have also been installed in the Joint Air Defense Operations Center (JADOC) at Boling AFB that provide air defense for NCR.

In January 2004, MSCT and TDF were deployed to the Baghdad International Airport to support the Control and Reporting Center (CRC) located in that theater. US Central Command (CENTCOM) requested this capability to fuse the sensors deployed in theater and then feed that information into the CRC. This gave the CRC an enhanced air picture with greatly extended range within the theater. The MSCT and TDF were deployed in a mobile transient case configuration. Figure 10 shows the MSCT and TDF located in a tent in Baghdad, Iraq [3]. This is another example of how the components of the TCN architecture can be integrated into a system or used independently. Now that the initial architecture has been installed, it can be enhanced as user's needs increase or funding becomes available without the necessity to redesign the architecture.

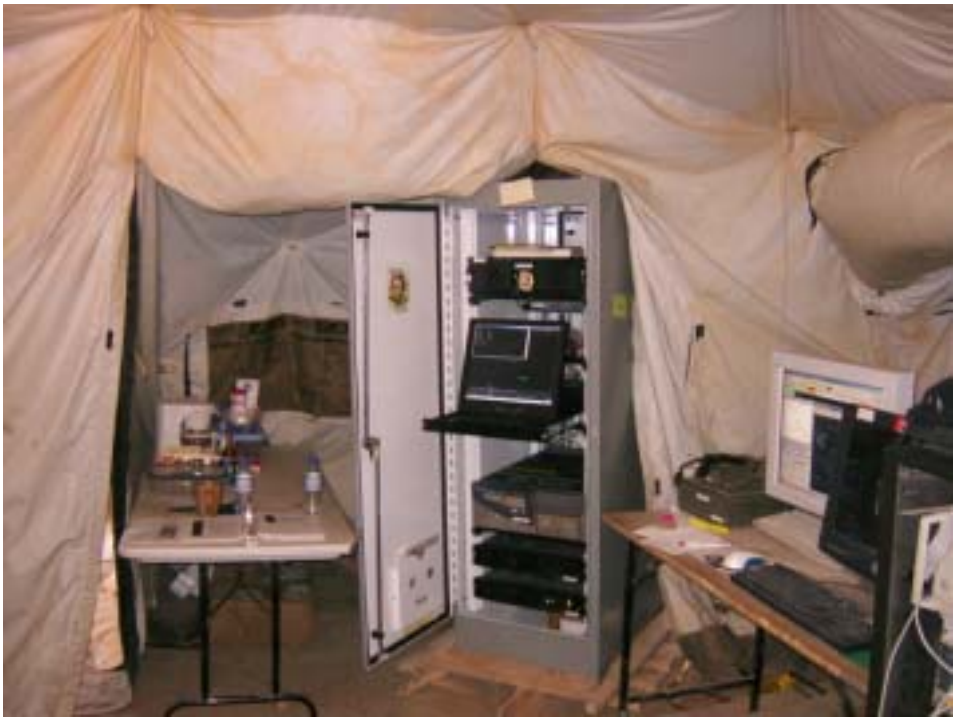


Figure 10 - MSCT and TDF Deployed in Iraq

Conclusions

As the scope of terrorist activities continue to expand, it is imperative that nations join together in a consolidated effort to detect and neutralize terrorists before they can execute their plans. This can only be accomplished by networking and sharing information in a collaborated fashion; these networks must allow for the sharing of high fidelity information without compromising sources. Terrorist actions and methods will continue to adapt to the environment, so it is critical that networks also adapt to meet those challenges. TCN provides a network architecture that combines advantaged users with disadvantaged users in an integrated secure network, establishing "mission-centric" networks that can be scaled immediately to meet the changing environment. Figure 11 demonstrates that the capabilities for TCN International Operations are available today for immediate fielding to support the war on terrorism.

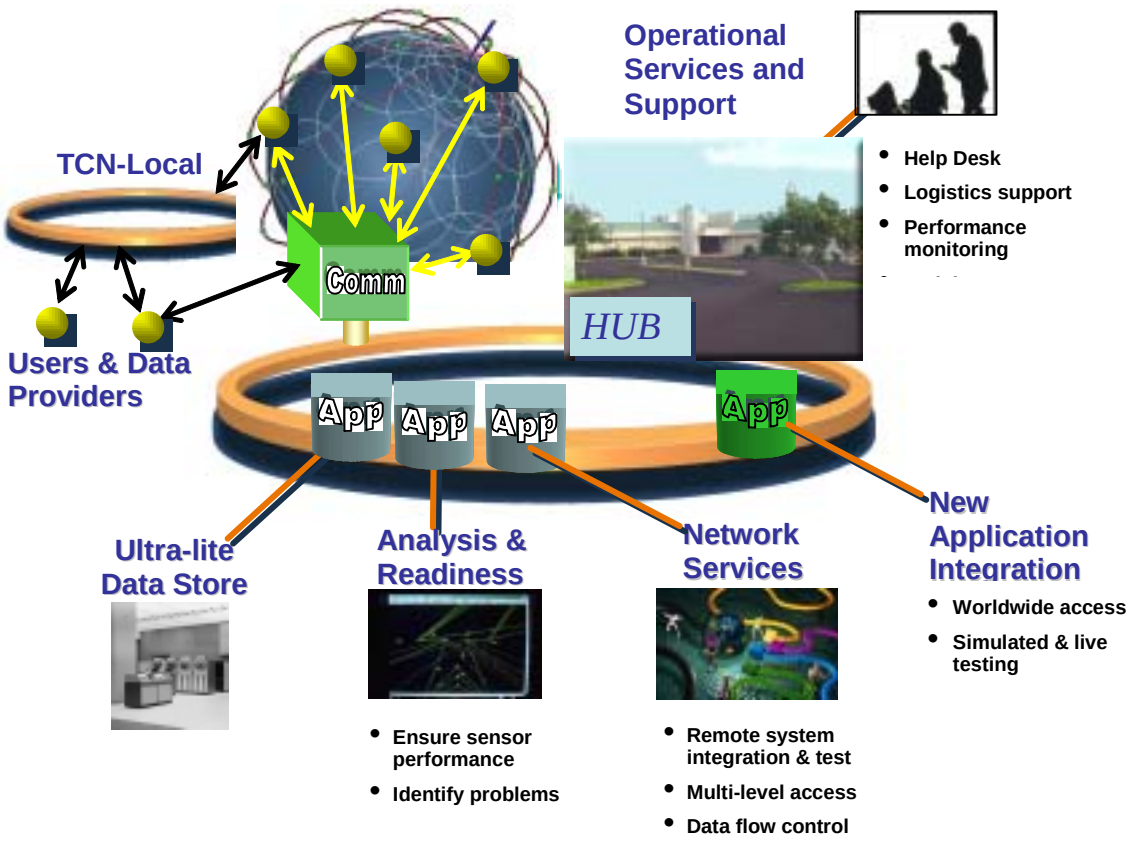


Figure 11 - TCN International Operation

References

[1] Raytheon Solipsys, “TCN White Paper”, (12 December 2003)

[2] Mike Abrams, David Buscher, Paul Giaccio, and Bob MacKenzie, “Tactical Component Network (TCN) – An Enabling Network-Centric Technology for Homeland Defense”, Government Microcircuit Applications & Critical Technology Conference (GOMAC), April 2003, Tampa, FL.

[3] Eric Firkin and Margaret McMahon, “Architecture for a Truly Integrated Defense Network”, to appear in the 2004 Command and Control Research and Technology Symposium (CCRTS), San Diego, June 2004.

[4] Margaret McMahon. "A Hub-and-Spoke Network for Global Network-Centric Applications", accepted by PDPTA'04, Las Vegas, NV, June 2004.

[5] Margaret McMahon, and David Buscher, "A Hub-and-Spoke Architecture for Netcentric Operations (Urban Security)", Government Microcircuit Applications & Critical Technology Conference (GOMAC), April 2003, Tampa, FL, paper 09-04.

[6] Eric Conn, Steve Lee, Eric Firkin, and David Buscher, “NORAD Contingency Suite (NCS) – The Frontline in Homeland Air Surveillance and Defense”, Government Microcircuit Applications & Critical Technology Conference (GOMAC), April 2003, Tampa, FL.

Biographies

Eric C. Firkin is a former USAF Air Battle Manager with more than 24 years of experience in the Command and Control domain. He retired from the USAF in January 2003. During his career he served as a Commander, Director of Operations, and Mission Crew Commander in several units in the Ground Theater Air Control System (GTACS), which included deployments in South America, Southwest Asia, and the Korean peninsula. Prior to his retirement he served as Chief, C2 Operations and Systems Branch, Air Force Command and Control, Intelligence, Surveillance, Reconnaissance Center (AFC2ISRC, Langley AFB, VA where he was responsible for the modernization and sustainment of the GTACS community. He currently serves as the Director, USAF Business Development for Raytheon Solipsys and is responsible for all USAF Programs for the company.

Margaret McMahon has more than 22 years in defense engineering and defense-related activities. Her experience in aircraft systems specification and testing gives her practical insight into the issues facing incorporation of technology in a military environment. She has extensive experience in the engineering and testing of the F/A-18, AV-8B, and A-10A aircraft. This experience is from both Government and contractor perspective and has yielded numerous scholarly publications. While at the Naval Air Warfare Center in China Lake, she served as Advanced System Program Office Engineer, defining requirements for Special Programs using studies combining technology, tactics, and fleet realities. Her advanced systems studies involved leveraging these studies to quantify the benefits of future systems. As an Assistant Professor at the US Naval Academy, her research in network security has specialized in authentication and ad hoc networking. She teaches basic and advanced network courses to future Naval Officers. Dr. McMahon's current research involves the implementation of network-centric technologies and includes consultation for Raytheon Solipsys in both Laurel, MD, and Kauai, HI. In this capacity, she is responsible for defining requirements for global Tactical Component Network (TCN) and has developed use cases to demonstrate how this architecture would support Ship-to-Objective-Maneuvering (STOM) tactics.

Raytheon Solipsys

Network Centric Warfare for Coalition Integrated Defense Against Terrorism

September 2004

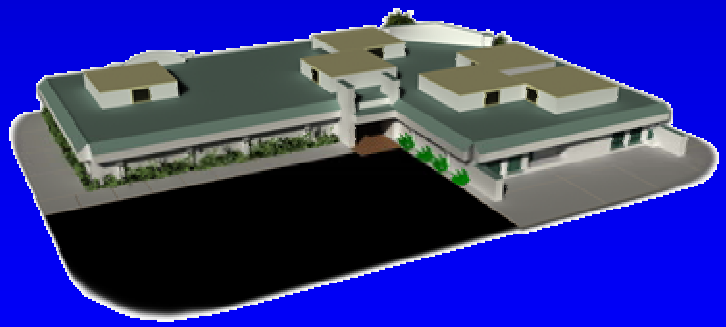
Eric C. Firkin
Director, USAF Business Development
Raytheon Solipsys Corporation

Margaret M. McMahon, Ph.D.
Computer Science Department, US Naval Academy

Corporate Overview

Raytheon Solipsys

- Founded in March 1996 by Senior Researchers at Johns Hopkins University/Applied Physics Lab
- Core Business is the Design and Development of C4ISR Software Products for Military Use
- 165 Employees and Growing
- Headquarters in Laurel Maryland, Offices in Kauai, HI and Norfolk, VA
- Specializing in Network-Centric Warfare and C2 Systems
- Over 50 Percent of Staff have Advanced Engineering Degrees (MS or PhD)
- Merger with Raytheon made Solipsys a Wholly-Owned Subsidiary in 2003



Problem…

Raytheon Solipsys

- Challenge: to provide an integrated international, real-time sensor information dissemination system to defend against terrorism
  - Multiple governments, jurisdictions, organizations
  - Multiple networks with restricted collaboration
  - Myriad of encryption systems
  - Limited and diverse communications
  - Intelligence Boundaries
  - Real-time data distribution
  - Distributed Command Authority

Solution…

Raytheon Solipsys

Tactical Component Network (TCN)

- A software application suite for real-time sensor collaboration that provides:
  - Open Architecture framework
    - Employs a well defined API that facilitates component based systems integration
    - Hardware independence allows for a scaleable application
  - Communications flexibility
    - Patented "Goal oriented" algorithms enable data exchange that eliminates redundant information, optimizing use of available bandwidth
    - Not tied to a specific radio or device
    - Extensible to multiple communication paths

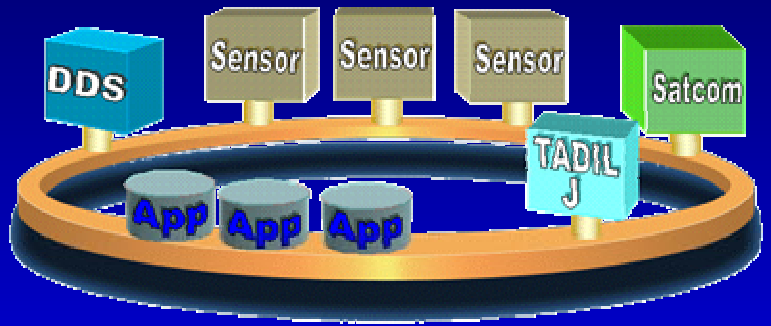
- Demonstrated and robust technology
  - Four years of lab, land-based and deployed test and assessment
  - Meets requirements ranging from target engagement to situation awareness
  - Demonstrated support for 3rd party component development

TCN Approach

Raytheon Solipsys

- Sensors and communications resources collaborate to form a Single Integrated Picture (SIP)
  - Data distribution based on user-defined accuracy requirements (smart pull vs push technique)
  - Data is created and delivered in a source independent form (supplier can be annonymous and users can be segregated based on a need to know)
  - Addition of new sensor, communications device or application program does not require change to other network participants (extensible, interoperable)

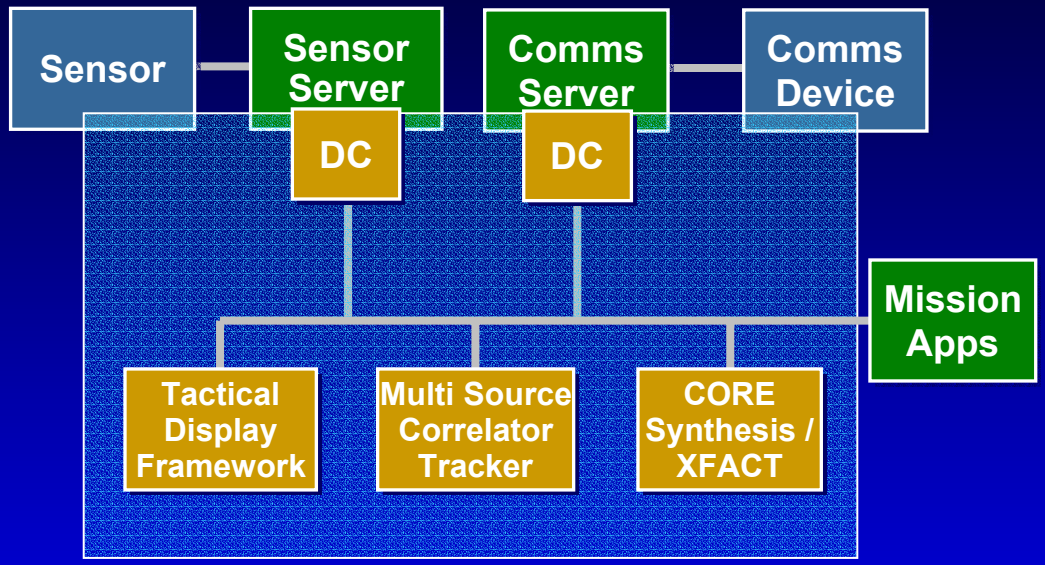
TCN Architectural Model



Supports both LOS and BLOS network operations, with seamless interconnectivity

- Supports simultaneous, real-time collaboration between Joint and Coalition network participants in support of the Global Information Grid (GIG)
- Incorporates and extends mission-centric network architectural concepts to meet users needs

TCN Architectural Components



- TCN Foundation Applications
  - Data Conditioner (DC): Data abstraction layer for sensors and comms devices
  - CORE Synthesis/XFACT: TCN fusion and collaboration
  - Tactical Display Framework (TDF): Battle management and C2 display
  - Multi Source Correlator Tracker (MSCT): Data link integration, legacy system interfaces, dissimilar source correlation and tracking
- Sensor Server, Comms Server, and Mission Apps (depicted in green) are developed by third party (e.g., LM for AEGIS, NG for E2C, Boeing for AWACS, etc.)

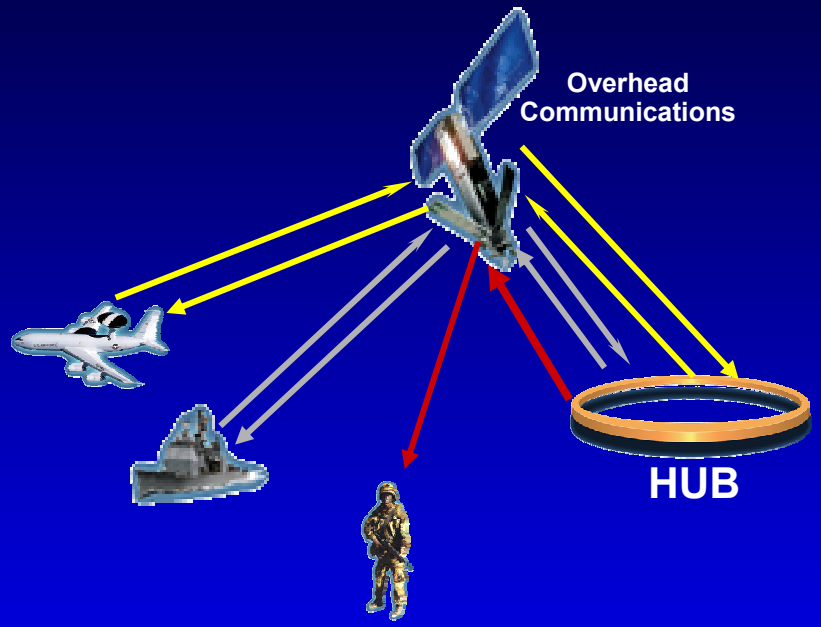
TCN – Coalition Military Application

Raytheon Solipsys

TCN Local Network

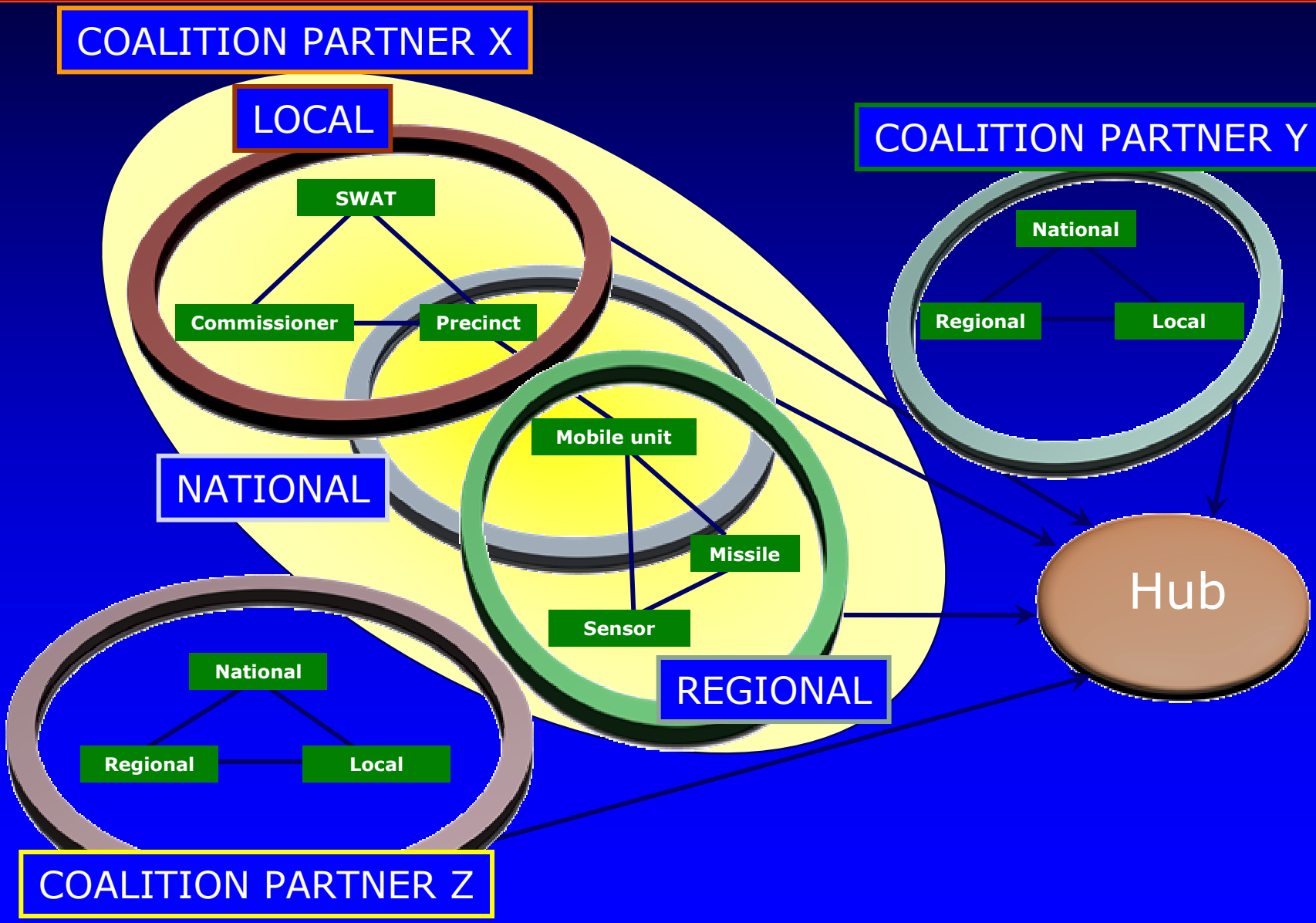
- Support time critical communications among peer-to-peer participants
- Aggregate bandwidth shared between participants based on user needs

TCN Global Network



- User connectivity is not constrained by Line of Sight - Global reachback
- Secure real-time data available via LEOs or other overhead assets
- Hub provides access control, database support, processing enhancements and central applications

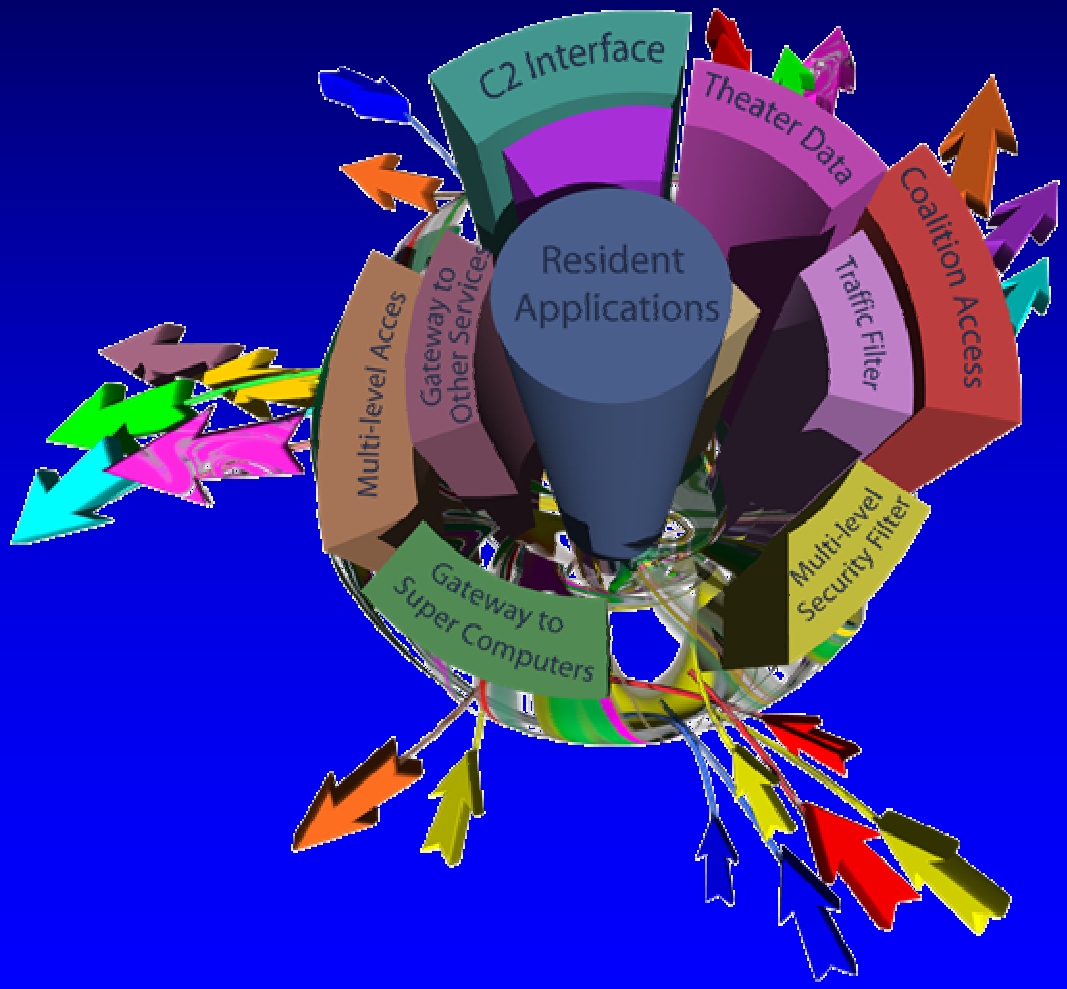
TCN Hub-and-Spoke Architecture



Hub Components/Functions

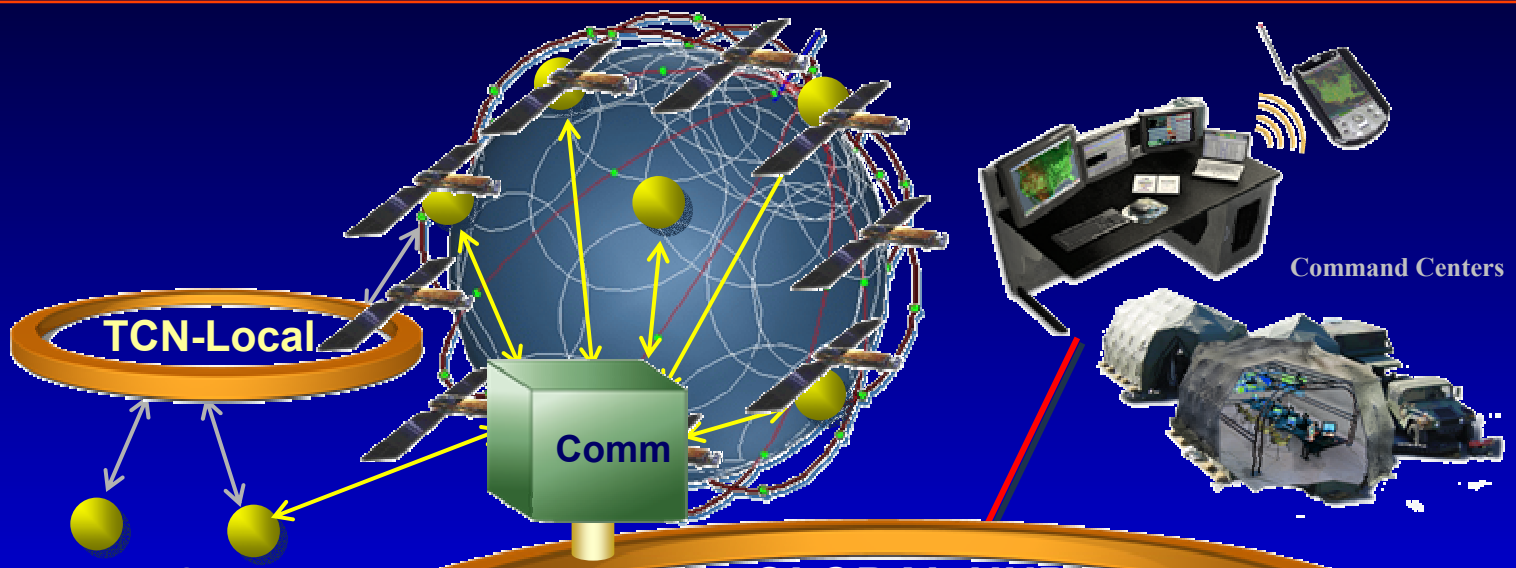
Raytheon Solipsys

- Operating System
- Connection Manager
- Database Managers
  - Theater Data
  - Geographic Data
  - Cultural Features
- Data Archive
- Access Control
  - Traffic
  - Multilevel Access
  - Coalition Access
- Gateway Management



TCN Local/Global Operation

Raytheon Solipsys



First Responder's

Interpol

Intelligence Sources

Air Traffic Control

NATO
OTAN

Coalition Partners

Military Air Picture

Summary

Raytheon Solipsys

- Solipsys specializes in high performance fully customizable COTS software components that can be used individually for point solutions (displays, correlators, simulation tools, etc.) or coupled together to form a complete hardware-independent C2 system appropriate for each echelon of command

- Full TCN Brief available for download at: www.solipsys.com

Contact Information:
Eric “Frack” Firkin
Director, USAF Business Development
eric.firkin@solipsys.com
757-224-0612 (office)
757-615-1832 (mobile)